RECEIVED
CENTRAL FAX CENTER

APR 04 2006

MOTOROLA

FAX TRANSMITTAL SHEET

Motorola, Inc.
Intellectual Property Section
Law Department
101 Tournament Drive
Horsham, PA 19044

Telephone: 215-323-1000
Facsimile: 215-323-1300

4 Number of Pages (including this page)

Date: April 4, 2006

To: Minh Dihn – Group 2132

Location: United States Patent and Trademark Office

Fax No.: 571-273-8300

From: Robert P. Marley – No. 32,914

Subject: 09/898,136 – Annie On-yee Chen et al. DOCKET NO. D02570-04

MESSAGE:

PLEASE GIVE THESE PAPERS TO:

EXAMINER: **Dihn, Minh**
GROUP ART UNIT: 2132
Serial No.: 09/898,136
Filed: July 3, 2001
Inventor: Annie On-yee Chen et al.
Docket No.: D02570-04

RECEIVED
CENTRAL FAX CENTER

APR 04 2006

Docket No.: D02570-04

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Annie On-yee Chen Lawrence W. Tang Akkio Wakabayashi	GROUP ART UNIT:	2132
APPLN. NO.:	09/898,136	EXAMINER:	Minh Dihn
FILED:	July 3, 2001		
TITLE:	SYSTEM FOR DENYING ACCESS TO CONTENT GENERATED BY A COMPRIMISED OFF-LINE ENCRYPTION DEVICE AND CONVEYING CRYPTOGRAPHIC KEYS FROM MULTIPLE CONTIONAL ACCESS SYSTEMS		

Dear Examiner Dihn:

In response to your inquiry regarding support for two limitations of amended claim 1 in Application No. 09/898,136, I respectfully provided the references below. I have designated the "generating a unique key ..." limitation as CLAUSE 1, and the "encapsulating each of said unique keys ..." limitation as CLAUSE 2.

Amended Claim 1 reads as follows:

> 1. (Presently Amended) A method for use in cable systems, the method for forwarding messages containing cryptographic keys from multiple access sytems that control a population of set-top boxes to an encryption renewal system, the method comprising:
>
> storing a single fictitious address of a virtual set-top box, said fictitious address being identical for each of said multiple access systems;
>
> ***generating a unique key within each of said multiple access systems as a function of the identity of each particular access system; [CLAUSE 1]***
>
> encrypting said unique key for each of said multiple access systems;
>
> ***encapsulating each of said encrypted unique keys in a message encoded to be forwarded to said single fictitious address. [CLAUSE 2]***

In Paragraph 0009 of the originally filed application, support for CLAUSE 1 can be found in the italicized sentence –

[0009] In a first embodiment, the system of U.S. Ser. No. _____, includes a content preparation system (CPS) for pre-encrypting the content offline to form pre-encrypted content; an encryption renewal system (ERS) for generating entitlement control messages (ECMs) that allow the pre- encrypted content to be decryptable for a designated duration; and a conditional access system (CAS). ***Conventionally, the CAS controls a population of set-top boxes using a randomly generated periodical key.*** Only with possession of the periodical key can the pre-encrypted content be decrypted by the set-top boxes. The periodical key is initially forwarded to the ERS which thereafter generates an ECM containing information regarding the periodical key.

So periodical keys within cable encryption systems are uniquely generated random keys. Further support for the unique nature of the periodical key of the invention is found in paragraph 0075 of the originally filed application –

[0075] At block **308**, the method includes the step of receiving the EMM by ERS **202** which has information concerning the fictitious address. ERS **202** contains secure code and acts like a set-top to derive the clear periodical key from the EMM. The periodical key is typically buried inside the EMM. ***ERS 202 also contains database (not shown) which stores the periodical key associated with each CAS.*** In this fashion, upon receiving an EMM, ERS **202** retrofits the requisite ECM having the periodical key for forwarding to the appropriate cable system. Although not shown, one of ordinary skill in the art will realize that communication links **242**, **240** may comprise wired telephone line, fiber, satellite or radio frequency channel for example. In fact, no physical link may exist e.g. SneakerNet wherein the EMM is manually collected on a floppy disk and walked over to ERS **202**. The so- called SneakerNet provides the advantage of erecting a physical barrier between the components.

Clearly, if there is a periodical key associated with each individual CAS, the keys must be discernable from one another (i.e., unique).

As for support for CLAUSE 2, I again direct your attention to paragraph 0017 of the originally filed application –

> [0017] According to another aspect of the present invention, a method for use in a communication system is disclosed. The method is for forwarding messages containing periodical keys from one or more access systems that control a population of set-top boxes to an encryption renewal system. The method includes storing a fictitious address of a virtual set-top box; ***generating a first message based on the fictitious address, the message containing a first periodical key; and forwarding the first message to the fictitious address of the virtual set-top box***. In a further aspect, the method includes the encryption renewal system, which has knowledge of the fictitious address, receiving the first message.

The message being generated for transmission to the fictitious address contains (i.e., encapsulates) the periodical key (a.k.a., the unique keys).

It is hoped that this brief explanation provides sufficient evidence of proper support for the two limitations at issue.

I look forward to conferring with you upon your return to your office.

Respectfully,

Robert P. Marley
Reg. No. 32,914
Attorney for Applicants
(215) 323-1907